JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Nuances on Cybercrime with special reference to Data Diddling - A study

Dr.J.Star,M.L.,
Ph.D., Assistant Professor of Law, CDAGLC, Pattaraiperumbudur.

Abstract
The ingenuity of cyber criminals is becoming clear when we look at the clever ways in which online frauds are being perpetrated. cyber criminals combines elements of fake, falsification and lost trust to obtain sensitive personal data like credit card details, PIN numbers, passwords, etc. of victims. The attackers then cheat the victims by using such personal information. Other forms of cyber crimes include illegal access to data, hacking, alteration of information and E-mail based offences. Data diddling is an unauthorized altering of data before or during entry into computer system and changing it same after the processing is done. As the original information that is entered is changed either by the person typing the data, a virus that programmed to change the data, the programmer of the data base or the application, or anyone else is involved in the process of creating, recording, encoding, examining, checking, converting and transmitting data. It is said to be one of the simplest methods of computer related crime.

Introduction

Data Diddling is one of the most common forms of computer crime data diddling is an llegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory re-cords, credit records, school transcripts and virtually all other forms of data processing known.This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances. This paper mentioned about the ideas relating to one of the cyber crime data didiling in India.

Data Diddling meaning:

It is a type of cybercrime in which data is altered as it is entered into a computer system[1], most often by a data entry clerk or a computer virus[2]. Such Computerized processing of the altered data results in a fradulent benefit. In some cases, the altered data is changed back after processing to conceal the activity[3]. The results can be huge. They might include adjusting financial figures up or down marginally, or it could be more complex and make an entire system unusable[4]. Data diddling can occur at various points along the chain of information entry, and it is often very subtle and virtually undetectable. It can be something as small as a time clerk substituting his own name or employee number for another employee's name or number. It can be combated by ensuring that all information is identical, whether it is a hard copy or the data within a digital system[5].

1Romney, Marshall (1995). "Computer fraud--what can be done about it?". CPA Journal. 65: 30.

2"The 12 types of Cyber Crime" Digit. Retrieved October 1, 2018.

3Parker, Donn B. (1989), Computer Crime: Criminal Justice Resource Manual , (second edition), National Institute Justice, pp.12-13.

4Silverbug, "Ten types of Cyber Crimes and another Ten You've Never Heard of, available at www.silverbug.it. Retrieved 22.07.2023.

5Hébert, Monique; Pilon, Marilyn (1991), Computer Crime, Law and Government Division, Library of Parliament.

Background of the study:

As it is said to be one of the easiest crimes to commit so it will be said as effortless task, it can have detrimental effects. For example, Electricity boards in India have victims of data diddling by computer criminals when private parties were computerizing their systems.As Data diddling is also refers to changing of data before or during entry into the computer system[6]. This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. The NDMC Electricity Billing Fraud Case[7] that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and payment in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

Data Diddling is a Cybercrime:

A cybercrime where a person intentionally enters wrong information into a computer, system, or document. It is often used when businesses and individuals want to hide part of their profits for tax evasion purposes. It could also be used to do the opposite - fabricate the average order value or the number of sales to make it look like the business has more customers than it really does. This is done to get a better loan proposal from the bank. If a business owner wants to brings their competitors down, they can also use this technique to cause damage to someone's company or its reputation[8]. Data diddling can be performed by someone whose job it is to enter the data or remotely by hacking the system or using malware to automatically change input data. While most cybercrime involves compromising or stealing data that has already been entered, data diddling refers to compromising raw data at the entry point, just before it is processed by a computer or a system[9].

Data Diddling under Indian Law:

In India, alteration of data available in computer resource or diminishing its value or utility or affecting it injuriously so as to cause wrongful loss or damage to the public or any person would be an offence punishable under Section 66 of the IT Act. Such kind of computer crime would also be comes under offences mentioned under Section 43(d) of the IT Act. If anyone commits an ofence of data diddling in India, he is liable to be punished for the offence under Section 43(d)[ii] readwith Section 66 [i] of the I.T. Act and the punishment for the offence as mentioned under this Act is fine not increasing one Crore Rupees.

Related Case Laws:

The famous case which is relating to data diddling is NDMC Electricity Billing Fraud Case. In this case, a private contractor who was to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerised, accounting record maintenance and remittance in his bank who misappropriated huge amounts of funds by manipulating data files to less receipt and bank remittance.

Controlling measures on Data Diddling:

To take certain precautions while using the internet. So always follow these preventive approaches- Be aware that your mobile device is vulnerable to viruses and hackers. To download the applications from trusted sources alone. Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location Use of firewalls may be beneficial[10]. Always use secure wireless network. The Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi's are played a vital role for the commission of such type of crimes. Since to avoid conducting financial or corporate transactions on these networks. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

6Parker, Donn B. (1989), Computer Crime: Criminal Justice Resource Manual , (second edition), National Institute Justice, pp.12-13.

7Adwel Advertising (P) Ltd. v. N.D.M.C. and another, 2003 IIAD Delhi 452.

8Hébert, Monique; Pilon, Marilyn (1991), Computer Crime, Law and Government Division, Library of Parliament.

9Brandt Allen, "Embezzler's Guide to the Com-puter," Harvard Business Review, p. 53 (July 1975).

10Silverbug, "Ten types of Cyber Crimes and another Ten You've Never Heard of, available at www.silverbug.it. Retrieved 22.07.2023.

Protection from data diddling:

To protect themselves from data diddling, businesses should use antivirus software to guard their networks, systems, and devices from viruses. It's essential to have proper training and access management protocols in place to minimize insider threats. Managing sensitive financial information should require additional authentication where more than one person's approval is necessary for making changes or inputting important data. This computer crime relates to operation security and is minimized through strengthening of internal security controls. This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed[11]. This is a simple and common computer related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data[12].

Conclusion:

Cyber crimes can involve criminal activities such as mischief, theft, fraud, forgery and offense all of which are subject to the Indian Penal Code. False data entry is usually the simplest, safest, and most common method used in computer abuse. It involves changing data before or during their input to computers. Anybody associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer can change these data. Trusted, authoriz-ed computer users engaged in unauthorized activities are often the persons using the method. Examples of data diddling are forging, misrepresenting, or counterfeiting documents; by way of exchanging valid computer tapes or disks with prepared replacements, keyboard entry falsifications, failure to enter data, and neutralizing or avoiding controls. To take effective steps to enable students to secretly report acts of harassment to teachers and school administrators and require students to be notified annually of the process by which they may report. Require teachers and other school staff who witness acts of harassment or receive student reports of bullying to notify school administrators in writing. Enable the parents or guardians of students to file written reports of suspected harassment.

11Donn B. Parker, Fighting Computer Crime (Charles Scribner's Sons, New York, New York, 1983).
12Brandt Allen, "Embezzler's Guide to the Com-puter," Harvard Business Review, p. 53 (July 1975).